U.S. DEPARTMENT OF COMMERCE

UNITED STATES PATENT AND TRADEMARK OFFICE

Privacy Impact Assessment

Personal Identity Verification System
Card Management System

(HSPD12-PIVS/CMS)

January 18th, 2011

Privacy Impact Assessment

This Privacy Impact Assessment (PIA) is a requirement of the Privacy Act of 1987 and OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.* A PIA documents the due diligence and oversight placed upon information associated with the project or system in question. Written from the System Owner's perspective for the American public, the PIA discloses what information is being collected, and how that information is protected. The intent is to build confidence that privacy information is secure, processes that utilize this information comply with Federal requirements, and more importantly, inform the privacy expectations of the American public.

The Privacy Threshold Analysis (PTA) is a separate artifact that must be completed prior to beginning this PIA. In many cases, the PTA will be the only required artifact to satisfy DOC privacy considerations.

SYSTEM DESCRIPTION

Part I. Project Identification and Determination of PIA Requirement

1. **PROJECT IDENTIFICATION:**

1.1) **Project Basic Information:**

1.1.a) *Project or Application Name:*

HSPD-12 Implementation: Personal Identification Verification II (PIVS II)

1.1.b) *OMB Unique Project Identifier*: **N/A**

1.1.c) *Project Description*

Project description is pre-populated from Exhibit 300 Part I.A.8. You will not be able to edit the description on this form.

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (HSPD-12) was issued on August 27, 2004. HSPD-12 directed a new Federal standard for secure and reliable identification to be issued by Federal agencies for their employees and contractors. The National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201-Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201) on February 25, 2005. The USPTO PIV Program evolved from the United States Patent & Trademark Office existing Credentialing Program. One of the objectives of USPTO PIV Program was to establish an enterprise and standards-based authentication and authorization infrastructure framework that would support secure and seamless transmission of business transactions and information within USPTO and to USPTO business and operational partners, through the use of smart card technology and Public Key Infrastructure ((PKI)). After the release of HSPD-12 and FIPS 201, a decision was made to implement a USPTO PIV program and requested that the agency, should be allowed to, on its own, provide the infrastructure required to implement secure logical and physical access. The initial conceptual approach for the USPTO PIV System was to build upon the existing PKI infrastructure by adding required functionality and services to achieve compliance with HSPD-12 and FIPS 201. Each service within the USPTO PIV System is wrapped with web services and delivers services over well defined interfaces. The services required within the PIV solution include:

- **Enrollment .**
- **Identity and Access Management .**
- **Security .**
- **Data Support .**
- **Publication .**
- **Audit .**
- **Archive .**
- **Secure Data Storage .**
- **Human Machine Interfaces .**

- **Card Management .**
- **Public Key Infrastructure**

1.1.d) *Additional Project Information (Optional)*
The project description provided above should be a concise, stand-alone description of the project. Use this section to provide any important, supporting details.

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors" (HSPD-12) was issued on August 27, 2004. HSPD-12 directed a new Federal standard for secure and reliable identification to be issued by Federal agencies for their employees and contractors. The National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201-Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying personal identity verification (PIV) cards for their employees and contractors. The USPTO PIV Program established a fully functional and compliant USPTO Personal Identity Verification System (USPTO PIV System) responsible for the issuance and management of PIV Cards. The USPTO PIV Program evolved from the from the United States Patent & Trademark Office existing credentialing program. One of the objectives of USPTO PIV Program was to establish an enterprise and standards-based authentication and authorization infrastructure framework to support secure and seamless transmission of business transactions and information within USPTO and to USPTO business and operational partners, through the use of smart card technology and Public Key Infrastructure (PKI). After the release of HSPD-12 and FIPS 201, a decision was made to replace the existing credentialing efforts with the USPTO PIV program. FIPS 201 consists of two parts. The first part defines specific roles and processes while the second part defines technical requirements. The USPTO PIV program implemented Part I of FIPS 201 from April 2006 until the start of PIV II issuance (expected in April 2010). The program disseminated guidance and implemented the FIPS 201 PIV card processes throughout the agency and achieved compliance with the Presidential mandate within the stipulated deadlines. Implementation of Part II of FIPS 201 began in May of 2008. The initial conceptual approach for the USPTO PIV System was to build upon the existing PKI Infrastructure by adding required functionality and services to achieve compliance with HSPD-12 and FIPS 201. The USPTO PIV Program established an engineering approach for the USPTO PIV System which embraced Services Oriented Architecture (SOA). The SOA approach leveraged web-services and standards based interfaces to accomplish four objectives: . Utilize the PKI solution to build a transitional PIV solution that is compliant with federal guidelines and the PIV II implementation date. Permit the build of an incremental solution that achieves compliance with HSPD-12 and FIPS 210 in phases. . Allow for a decoupling of USPTO PIV System component integration and employ a model of supplier and consumer services consistent with industry best practices. Provide a means to leverage the services of the USPTO PIV System into an Enterprise vision of identity and access management, making the both solution forward-looking and Enterprise capable. Integrate PIV System services into an identity and access management solution that

supports the needs of the USPTO Enterprise. USPTO integrated a test region for the USPTO PIV program to provide the architectural baseline that will carry forward into subsequent phases of the program. The USPTO PIV Program is currently implementing the second phase of implementation, with an expected delivery date of 04/2010. This phase of the system implementation provides the USPTO with the fully compliant PIV Solution, dubbed the USPTO PIVS II System version 1.0. The USPTO PIVS II System will incorporate elements in the production system that include the biometric services, the Oberthur PIV Card stock, and the supporting workflow and digital signature processes that will provide the USPTO with a fully compliant PIV solution, as well as embrace the requirement of the Government Paperwork Elimination ACT (GPEA) through the implementation of a fully electronic enrollment process. All transactions within the system that are required under FIPS 201-1 for enrollment of Card Applicants for PIV Cards will accomplished with electronic forms that apply PKI based digital signatures, thus eliminating the need for any paper forms within the deployed solution. Certification and Accreditation: The program will certify and accredit the USPTO PIV System in accordance with USPTO direction and NIST SP 800-53 guidance.

1.2) **Contact Information:**
1.2a) **Person completing this document:**

1.2a Person Completing Document	
Title:	Joseph Burns
Organization:	USPTO PIV Project Manager
Telephone Number:	571-272-1537
Email Address	joseph.burns@uspto.gov
1.2.b) Project Manager:	Joseph Burns
Title:	USPTO PIV Project Manager
Organization:	Office of Security Operations
Telephone Number:	571-272-1537
Email Address	joseph.burns@uspto.gov
1.2.c) Staff Contact Person	Joseph Burns
Title:	USPTO PIV Project Manager
Organization:	Office of Security Operations
Telephone Number:	571-272-1537
Email Address	joseph.burns@uspto.gov

ADDITIONAL INFORMATION: If appropriate, provide explanation for limited answers, such as the development stage of project.
A privacy impact assessment (PIA) is required for all USPTO projects with IT systems that collect, maintain, and/or disseminate personally identifiable information (PII) of the public, not including information of Federal employees and others performing work for USPTO (such as contractors, interns, volunteers, etc), unless it is a PIV II project. All PIV II projects collecting any PII must complete a PIA. PII is any representation of information that permits the identity of an individual to be reasonably inferred by either direct or indirect means. Direct references include: name, address, social security number, telephone number, email address, financial information, or other identifying number or code. Indirect references are any information by which an agency intends to identify specific individuals in conjunction with other data elements. Examples of indirect references include a combination of gender, race, birth date, geographic indicator and other descriptors.

2. a) Will the project collect and/or maintain personally identifiable information of the public in IT systems?
No.

2. b) *Is this a PIV project collecting PII, including from Federal employees, contractors, and others performing work for USPTO?*
Yes.

If "Yes" to either question then a PIA is required for this project. Complete the remaining question on this form. If "NO" to both questions then no PI is required for this project. Skip to section 13 and affirm.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section)

PIVS II information systems will only collect, maintain, and/or disseminate Personally Identifiable Information of Federal employees and others performing work for USPTO (such as contractors, interns, volunteers, etc.). Although the e-Gov Act of 2002 specifically requires PIAs for IT systems that collect, maintain, and /or disseminate Personally Identifiable Information of the public, it does not include information of Federal employees and others performing work for USPTO (such as contractors, interns, volunteers, etc). However, OMB specifically requires the completion of PIA to meet the privacy requirements of FIPS 201-1.

PART II. PRIVACY IMPACT ASSESSMENT

3. **PROJECT DESCRIPTION:**
Enter the information requested to describe the project.
3.a) Provide a concise description of why personal information is maintained for this project
Personal information of employees, contractors, volunteers and affiliates will be collected and maintained from those requesting USPTO identification badges, in accordance with HSPD-12 mandate and related FIPS 201-1 privacy data collection requirements. The goal of the PIV System is to achieve compliance with HSPD-12 and FIPS 201-1.

Within the context of this goal, the system intends to provide:

- **Personal Identity Verification (PIV) cards based on secure and reliable forms of identification credentials.**
- **Issuance of PIV Credentials based on validation of an individual's true identity and validation of the organization affiliation.**
- **PIV credential holder Identity Management., Access Management and security policy enforcement surrounding the PIV processes.**
- **PIV Credential enrollment, registration, issuance and lifecycle management automation.**

3.b) *What specific legal authorities authorize this project, and the associated collection, use, and/or retention of personal information?*
In accordance with HSPD-12 and FIPS 201-1, personal data such as fingerprints, personal information, and facial images will collected and stored for issuing PIV cards to federal employees and contractors, and for conducting PIV card lifecycle maintenance functions. The biographic and biometric information collected will be used to conduct a criminal history records check via fingerprints. The fingerprints will be used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed on the PIV Card as a means to identify the cardholder. Biometric minutiae data will be deposited onto secure containers within the PIV Cards in accordance with the requirements from FIPS 201-1 and NIST SP 800-76. Any biometric information that is collected from the PIV solution will be immediately and securely stored on Probaris servers (which are located in the USPTO secure data center) once the PIV Cards are manufactured and provided to the Card Applicants. The USPTO PIV System will not store biometric information that pertains to Card Applicants for any period of time longer than is required to manufacture and maintain the PIV Card, in order to minimize security exposure that is associated with storing privacy data and the Agency’s System of Record. Further, any biometric information that is stored on the PIV Card is controlled and safeguarded by the actual smart card device, and the security boundaries that are associated with those tokens. The risk assessments and technical solution provided by these PIV Card products has been fully assessed and/or tested by the NIST and GSA and they have been approved by those agencies as acceptable for Federal Government use. The USPTO will utilize the products

that are published within the GSA Approved Product List (APL), which signifies that these devices are secure and provided only the necessary and approved interfaces to access privacy related data. Lastly, the personal information that pertains to a specific Card Applicant is secured by a full Role Based security model that is in place within the USPTO PIV System, and has been properly assessed and approved as part of the certification and accreditation process. This signifies the USPTO PIV System as a security system that has undergone rigorous assessment and testing, and that the environment provides the proper security controls to safeguard any personal information that is gathered for a Card Applicant

3.c*) Identify, by selecting the appropriate range from the list below, the approximate number of individuals that (will) have their personal information stored in project systems.*
There will be between 8,000-12,000 individual's identities stored on the Probaris system.

3.d) *Identify what stage the project/system is in: (1) Design/Planning, (2) Development/Implementation, (3) Operation/Maintenance, (4) Disposal, or (5) Mixed Stages.*
As of March 2010, the USPTO is currently in mixed stages (1, 2, and 3).

(2) Development/Implementation
3.e) *Identify either the approximate date (MM/YYYY) the project/system will be operational (if in the design or development stage), or the approximate number of years that the project/system has been in operation.*
Fully PIV-compliant cards were issued beginning 05/2010

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

4. SYSTEM OF RECORDS:
The Privacy Act of 1974 (Section 552a of Title 5 of the United States Code) and USPTO policy provide privacy protections for employee or customer information that USPTO or its suppliers maintain in a System of Records (SOR). A SOR is a file or application from which personal information is retrieved by an identifier (e.g. name, unique number or symbol). Data maintained in a SOR must be managed in accordance with the requirements of the Privacy Act and the specific provisions of the applicable SOR Notice. Each SOR Notice is to be published in the Federal Register. See "USPTO Handbook" , for additional information regarding Systems of Records.

4.a) Will the project or application retrieve personal information on the basis of name, unique number, symbol, or other identifier assigned tothe individual? If "No" then skip to section 5, 'Data Collection'.
Yes

4.b) Are the project and/or system data maintained under one or more approved System(s) of Records? IF "No" then SKIP to question 4.c.
Yes

4.b.1) For each applicable System of Records, list:
(1) The System of Records identifier (number),
N/A

(2) The name of the System of Records, and
Police and Security Records
Commerce PAT-TM-18 USPTO Identification and Security Access Control Systems

(3) Provide the location where the specific applicable System of Records Notice(s) may be accessed (include the URL).
http://www.gpo.gov/fdsys/pkg/FR-2008-10-23/pdf/FR-2008-10-23.pdf

IMPORTANT: For each applicable System of Records Notice that is not accessible via a URL: (1) Provide a concise explanation of why the System of Records Notice is not accessible via a URL in the "Additional Information" field at the end of this section, and (2) Send a copy of the System of Records Notice(s) to the Privacy Service.

4.b.2) Have you read, and will the application comply with, all data management practices in the System of Records Notice(s)?
Yes

4.b.3) Was the System(s) of Records created specifically for this project, or created for another project or system?
The SORN was created specifically for this project

If created for another project or system, briefly identify the other project or system.

4.b.4) Does the System of Records Notice require modification?
No
If "No" then skip to section 5, 'Data Collection'.
4.b.5) Describe the required modifications.
Not Applicable

4.c) If the project and/or system data are not maintained under one or more approved System(s) of Records, select one of the following and provide a concise explanation.
Not Applicable

Explanation: ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

5. **DATA COLLECTION:**

5.1 **Data Types and Data Uses**

Identify the types of personal information collected and the intended use(s) of that data:

a) Select all applicable data types below. If the provided data types do not adequately describe a specific data collection, select the "Other Personal Information" field and provide a description of the information.

b) For each selected data type, concisely describe how that data will be used.
Important Note: Please be specific. If different data types or data groups will be used for different purposes or multiple purposes, specify. For example: "Name and address information will be used to communicate with individuals about their benefits, while Name, Service, and Dependent's information will be used to determine which benefits individuals will be eligible to receive. Email address will be used to inform individuals about new services as they become available."

Yes Primary Subject's Personal Contact Information (name, address, telephone, etc.)

Specifically identify the personal information collected, and describe the intended use of the information.

Personal contact, biometric, and biographic information for applicants of a PIV credential (USPTO identification badge), such as employees, contractors, volunteers and other affiliates will be collected.

The purpose of collecting this information is to issue a PIV badge to an authorized individual. The biographic and biometric information collected will be used to conduct a background investigation that includes a criminal history record check. The fingerprints will used to verify identity of the holder of the credential and the photograph will be collected so that it can be printed o the PIV Card as a means to identify the cardholder. Intended use of the data is to identify and validate an employee's biographic data in order to issue them a valid government PIV card which contains pertinent applicant data required by FIPS 201-1, such as name, agency, photo image, etc.

Other than information to be printed on the actual PIV card, PIV credential applicants may be required to submit additional personal information - outside of the PIV enrollment process-regarding their personal background/employment history as part of the employment application process.

Applicant Information Collected for PIV Card Sponsorship:

- **Organization**
- **Agency Name**
- **First Name**
- **Middle Initial**
- **Last Name**
- **Suffix**

- **Email Address**
- **UPN**
- **Birth Date**
- **Citizenship Code**
- **USPTO Employee ID Number**
- **Name of Specialist (Sponsor)**
- **New Hire (Yes or No)**
- **Emergency Response Official (Yes or No)**
- **Employee Affiliation**
- **BI Investigation (Yes or No)**
- **Date BI Completed**
- **BI Result**
- **BI Type**
- **BI Completed By**
- **BI Comments**

Other Personal Information of the Primary Subject
Specifically identify the personal information collected, and describe the intended use of the information.
None

Medical Information
Specifically identify the personal information collected, and describe the intended use of the information.
None

Criminal Record Information
Specifically identify the personal information collected, and describe the intended use of the information.
FBI Criminal Fingerprint check results will be obtained as a part of the HSPD-12 card processing, but this information will NOT be stored or maintained in this system.

Education Information
Specifically identify the personal information collected, and describe the intended use of the information.
None

Other Personal Information
The "Other Personal Information" field is intended to allow identification of collected personal information that does not fit the provided categories. If personal information is collected that does not fit one of the provided categories, specifically identify this information and describe the intended use of the information.

No

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)
No

5.2 Data Sources
Identify the source(s) of the collected information.
a) Select all applicable data source categories provided below.
b) For each category selected:
i) Specifically identify the source(s) - identify each specific organization, agency or other entity that is a source of personal information.
ii) Provide a concise description of why information is collected from that source(s).
iii) Provide any required additional clarifying information.
Your responses should clearly identify each source of personal information, and explain why information is obtained from each identified source. (Important Note: This section addresses sources of personal information; Section 6.1, "User Access and Data Sharing" addresses sharing of collected personal information.) Note: PIV projects should use the "Other Source(s)" data source.

Public Sources:
Specifically identify the personal information collected, and describe the intended use of the information.
None
USPTO Files and Databases:
Other Federal Agency Source(s)

i) Specifically identify each Federal Agency that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.
Within the PIV process, Sponsors will submit information to OPM using the OPM provided tools (e.g., the EQIP system) to perform a Background Investigation as part of the hiring process. The PIV process has a dependency for a process for successfully adjudicate a fingerprint submission prior to issuing a PIV Card to a Card Applicant. The USPTO PIV System relies upon the results of the fingerprint submission process as a trigger to allowing or disallowing a PIV Card to be issued. Under certain circumstances when a federal employee transfers from another agency, evidence of a background investigation etc. could be supplied by a former agency to the USPTO Office of Security, which can verify through Office of Personnel Management background investigative historical databases.

State Agency Sources
Specifically identify the personal information collected, and describe the intended use of the information. - **None**

Local Agency Source(s)

i) Specifically identify each Local Agency (Government agency other than a Federal or State agency) that is a source of personal information. ii) Provide a concise description of why information is collected from each identified source. iii) Provide any required additional, clarifying information.

None

Other Sources:

i) If the provided Data Source categories do not adequately describe a source of personal information, specifically identify and describe each additional source of personal information. ii) For each identified data source, provide a concise description of why information is collected from that source. iii) Provide any required additional, clarifying information. USPTO employees, contractors and affiliates, via the USPTO xxxx form, for the purposes of issuing an ID badge. ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

None

5.3 Collection Methods

Identify and describe how personal information is collected: a) Select all applicable collection methods below. If the provided collection methods do not adequately describe a specific data collection, select the "Other Collection Method" field and provide a description of the collection method. b) For each collection method selected, briefly describe the collection method, and provide additional information as indicated.

Web Forms:

Yes. Information collected on Web Forms and sent electronically over the Internet to project systems.

Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.") Identify the URL(s) of each Web site(s) from which information will be submitted, and the URL(s) of the associated privacy statement. (Note: This question only applies to Web forms that are submitted online. Forms that are accessed online, printed and then mailed or faxed are considered "Paper Forms.")

The PIV enrollment process employs a Web-based enrollment portal that supports secure session connectivity (e.g., SSL v3.0/TLS v1.0) to infrastructure that is located in USPTO Data Centers. The infrastructure consists of web server platforms that are secure, certified and accredited and operated in physically secure environments at the data center locations. The portal is located on the
USPTO Intranet at https://w-hspd12-500.etc.uspto.gov/ID/Login.aspx

Paper Forms:

Yes. Information collected on Paper Forms and submitted personally, submitted via Postal Mail and/or submitted via Fax Machine.

Identify and/or describe the paper forms by which data is collected. If applicable, identify standard USPTO forms by form number.
Information specific to the request for a PIV card is collected on USPTO Form 2238 for the manual processes that are supported under the FIPS 201-1 PIV 1 process. The electronic process employs electronic forms that are bulk uploaded or uploaded via the URL and apply PKI based digital signatures and no paper forms are involved in that process

Electronic File: information stored on one computer/system (not entered via a Web Form) and Transfer: transferred electronically to project IT systems
Describe the Electronic File Transfers used to collect information into project systems. (Note: This section addresses only data collection –how information stored in project systems is acquired. Sharing of information stored in project systems and data backups are addressed in subsequent sections.)
Authoritative and approved sources within the USPTO will need to send electronic fingerprint information to the FBI using the FBI Civil Applicant System (CAS). The USPTO PIV Enrollment Officer role is an approved source that can submit fingerprints using available tools connected to CAS, but these processes are not integrated with the USPTO PIV System and the System does not store any of these transactions. They are performed separate and apart from the USPTO PIV System.

Computer Transfer Device: **Yes**
Describe the type of computer transfer device, and the process used to collect information.
Offsite backup storage tapes are managed by the USPTO OCIO data center for securely storing collected privacy data in the same fashion that privacy data is stored offsite for backup purposes.

Telephone Contact: Information is collected via telephone. **No**

Other Collection Method: **Yes**
Information is collected through a method other that those listed above.
If the provided collection method categories do not adequately describe a specific data collection, select the "Other Collection Method" field and specifically identify and describe the process used to collect information.
Form SF 87: Fingerprints are taken electronically on the PIV enrollment fingerprinting machine. The fingerprinting machine will transmit an electronic copy in EFTS format of the fingerprints to OPM/FBI through a secure network connection. Copies of fingerprints are maintained locally in temporary cache memory until they are processed into EFTS format and transmitted to OPM/FBI. They are then discarded at the USPTO PIV enrollment site without being stored.

5.4 **Notice**

The Privacy Act of 1974 and USPTO policy requires that certain disclosures be made to data subjects when information in identifiable form is collected from them. The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

5.4.a) Is personally identifiable information collected directly from individual members of the public and maintained in the project's IT systems?
No

Note: If you have selected NO above, then SKIP to Section 5.5, 'Consent'.
5.4.b) Is the data collection mandatory or voluntary?
Voluntary.

5.4.c) How are the individuals involved in the information collection notified of the Privacy Policy and whether provision of the information is mandatory or voluntary?
While providing this information is voluntary, if personnel do not provide the requested information in whole or in part, USPTO may not be able to complete their investigation, or the identity and registration process, or complete it in a timely manner. Failure to provide the requested information may affect their placement or employment, and will affect their ability to obtain a permanent PIV card. If using a PIV credential is a condition of their job, not providing the information will affect their placement or employment prospects.

5.4.d) Is the data collection new or ongoing?
Ongoing

5.4.e.1) If personally identifiable information is collected online, is a privacy notice provided that includes the following elements? (Select all applicable boxes.)

Not Applicable- Privacy notice is provided on each page of the application.
Yes - A link to the USPTO Website Privacy Policy is provided.
Yes - Proximity and Timing: the notice is provided at the time and point of data collection.
Yes- Purpose: notice describes the principal purpose(s) for which the information will be used.
Yes - Authority: notice specifies the legal authority that allows the information to be collected.
Yes- Conditions: notice specifies if providing information is voluntary, and effects, if any of not providing it.
Yes Disclosures: notice specifies routine use(s) that may be made of the information.

5.4.e.2) If necessary, provide an explanation on privacy notices for your project:
The Personal Identity Verification (PIV) Card Issuance Privacy Notice will be posted in the Security Services Center where cards will be issued and it will also be posted on the USPTO Intranet Office of Security site under the HSPD-12 section.

5.4.f) For each type of collection method used (identified in Section 5.3, "Collection Method"), explain:

a) What the subjects will be told about the information collection.

b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.).

c) How a privacy notice is provided. Note: if PII is transferred from other projects, explain any agreements or understandings regarding notification of subjects.

Web Forms: **Yes**

Explain:

a) What the subjects will be told about the information collection.

b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.).

c) How a privacy notice is provided.

The PIV process employs a Web-based electronic enrollment form. The applicant, at the time of enrollment, will be verbally informed of the purpose of the collected data and will have the ability to obtain a privacy notice sheet. They will be notified how the collected data will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data. The information will also be put on the USPTO Office of Security Intranet site.

Paper Forms: **Yes**

Explain:

a) What the subjects will be told about the information collection.

b) How this message will be conveyed to them (e.g., written notice,electronic notice if a web-based collection, etc.).

c) How a privacy notice is provided.

The PIV process employs a Web-based electronic enrollment form. The applicant, at the time of enrollment, will be verbally informed of the purpose of the collected data and will have the ability to obtain a privacy notice sheet. They will be notified how the collected data will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data. The information will also be put on the USPTO Office of Security Intranet site.

Electronic File Transfer: **No**

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what *agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:*

a) What they will be told about the information collection?

b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)?

c) How a privacy notice is provided?

Computer Transfer Device: **Yes**

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to notify subjects regarding:

a) What they will be told about the information collection?

b) How the message will be conveyed (e.g. written notice, electronic notice if web-based collection, etc.)?

c)How a privacy notice is provided?

Information via this method is for backup purposes only - information is not collected from subjects via Computer Transfer Device.

Telephone: **No**

Explain:

a) What the subjects will be told about the information collection.

b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.).

c) How a privacy notice is provided.

Other Method: **Yes**

Explain:

a) What the subjects will be told about the information collection.

b) How this message will be conveyed to them (e.g., written notice, electronic notice if a web-based collection, etc.).

c) How a privacy notice is provided.

ADDITIONAL INFORMATION (Provide any necessary clarifying information or additional explanation for this section.)

The PIV process employs a Web-based electronic enrollment form. The applicant, at the time of enrollment, will be verbally informed of the purpose of the collected data and will have the ability to obtain a privacy notice sheet. They will be notified how the collected data will be used to create a PIV card, legal authority for doing so, and other uses of the collected data. In addition, the applicant signature page will identify they have read the privacy implications of the collected personal data, and understand the implications and purpose of the data. The information will also be put on the USPTO Office of Security Intranet site.

5.5 Consent For Secondary Use of PII:
The Privacy Act and USPTO policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

5.5.a) Will personally identifiable information be used for any secondary purpose?
Note: If you have selected No above, then SKIP to question 5.6, "Data Quality."
No

5.5.b) Describe and justify any secondary uses of personal information.
N/A

5.5.c) For each collection method identified in question 5.3, "Collection Method," describe:
1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary. 2) The opportunities individuals have to grant consent for particular uses of the information. 3) How individuals may grant consent.
Some examples of consent methods are: (1) Approved OMB consent forms and (2) USPTO Consent Form (USPTO Form). Provide justification if no method of consent is provided.

Web Forms:
Describe:

> *1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.*
> *2) Theopportunities individuals have to grant consent for particular uses of the information.*
> *3) How individuals may grant consent.*

N/A

Paper Forms:

Describe:

> *1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.*
> *2) Theopportunities individuals have to grant consent for particular uses of the information.*
> *3) How individuals may grant consent.*

N/A

Electronic File Transfer:
For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.

b) The opportunities individuals have to grant consent for particular uses of the information.

c) How individuals may grant consent.

N/A

Computer Transfer Device:

For electronic transfers of information, where this system is receiving the information from another system and is not collected from the primary information source, please explain what agreements are in place that govern the responsibilities of the system collecting information from the primary information source to provide the following:

a) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.

b) The opportunities individuals have to grant consent for particular uses of the information.

c) How individuals may grant consent.

N/A

Telephone Contact Media:

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.

2) The opportunities individuals have to grant consent for particular uses of the information.

3) How individuals may grant consent.

N/A

Other Media

Describe:

1) The opportunities individuals have to decline to provide information, for instances where providing information is voluntary.

2) The opportunities individuals have to grant consent for particular uses of the information.

3) How individuals may grant consent. ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

N/A

5.6 Data Quality

5.6.a) Explain how collected data are limited to required elements:

The PIV enrollment form is Web-based and/or electronic form based for batch upload. The standardized form has been approved by the USPTO for vetting a candidate PIV applicant. The Web-based portal data collection fields cannot be modified, added, or omitted during the PIV applicant enrollment procedures. In addition, all required fields

must be completed or be properly filled in for batch uploading in order for the enrollment process to be approved for the next steps leading to card issuance. The data collected from the Web-based enrollment process leads to card issuance data provisioning. The USPTO form data collection is to provide a digital signature corresponding to acknowledgement of both the electronic and web-based enrollment forms.

5.6.b) How is data checked for completeness?
The electronic Web-based portal of the USPTO HSPD-12-PIVS/CMS System will not allow a record to be entered and saved electronically by an individual unless all required fields are complete; a PIV card cannot be issued with an incomplete system record. Additionally, before an enrollment record is finalized, the sponsor or enrollment officer can review for completeness/correctness and check for errors and make the proper corrections. Enrollment services are provided via the We-based portal interface to the authoritative and administrative PIV roles.

5.6.c) What steps or procedures are taken to ensure the data are current and not out of date?
All PIV personnel records are considered current and up-to-date as long as the badge has not expired. Employees, contractors, volunteers and affiliates are required to update changes to their information in the event of name changes, etc. There are clearance procedures for employees leaving USPTO to ensure they are removed from systems. Contractors are also required as part of their contracts to return issued badges when expired or at the end of the contract of ensure they are removed form the system. Both dates are accommodated in the PIV system with the revocation of the contractor certificates active on the card which grant them logical and/or physical access privileges until termination. Managers of volunteers/interns that were provided PIV badges are required to collect badges upon conclusion of work and return them to the issuer.

5.6.d) How is new data verified for relevance, authenticity and accuracy?
The Sponsor, Registrar, and Applicant will will verify new Applicant data sum bitted during PIV card lifecycle operations and maintenance functions, such as card renewal, charge in marital status, etc, using approved I-9 documents, and by signing the new data input, thereby approving the accuracy.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIA SECTIONS 6 - 13
Project Name
Personal Identification Verification-2009

6. Use and Disclosure

6.1 User Access and Data Sharing

Identify the individuals and organizations that have access to system data.
--> Individuals - Access granted to individuals should be limited to the data needed to perform their assigned duties. Individuals with access to personal information stored in project system must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to prevent as well as detect unauthorized access and browsing.
--> Other Agencies – Any Federal, State or local agencies that have authorized access to collected personal information must be identified, and documented assurance must be provided that appropriate policies and procedures are in place to protect personal information.
--> Other Systems – Information systems of other programs or projects that interface with the information system(s) of this project must be identified and the transferred data must be defined. Also, the controls that are in place to ensure that only the defined data are transmitted must be defined.
6.1.a) Identify all individuals and organizations that will have access to collected information. Select all applicable items below.

System Users	**Yes**
System Owner, Project Manager	**Yes**
System Administrator	**Yes**
Contractor	**Yes**

If contractors to USPTO have access to the system, describe their role and the extent of access that is granted to them. Also, identify the contract(s) that they operate under.

For the initial PIV deployment, USPTO contractors on the Probaris Inc. PIV contract who designed and integrated the PIV system into the USPTO enterprise will perform Tier II and Tier III maintenance operations and general administrative operations to the PIV system. Specifically, contractors supporting the deployment of the solution to the field will have access to the system to perform administrative operations and maintenance/set up operations. Designated contractors supporting the solution in USPTO Data Centers will perform administrative operations and maintenance operations. PIV contracts include: PIV Systems Compliance Integration and Implementation Services and Implementation and Training Support for the PIV Program.

For the actual enrollment and issuance phase of the PIV cards, the Security Services Center (SSC) uses contractors from Akima as part running the operational aspect of its badging services. With the rollout of HSPD-12, Akima contractors also serve as HSPD-12 Enrollment Officials and Issuance Officers.

Other Federal Government Agency
If information is shared with another Federal government agency(ies), identify the agency(ies). For each organization, identify the information that is shared and for what purpose.

OPM and FBI will be reviewing PIV applicant fingerprint data, as part of the background investigative process, for comparison against their database and return the results.

State Government Agency
If information is shared with a State government agency (ies), identify the agency (ies). For each organization, identify the information that is shared and for what purpose.
None

Local Government Agency
If information is shared with a local government agency (ies), identify the agency (ies). For each organization, identify the information that is shared and for what purpose.
None

Other Project/ System
If information is shared with other projects or systems:

1) Identify the other projects and/or systems, and briefly describe the data sharing.
2) For each project and/or system with which information will be shared, identify the information that will be shared with that project or system.
3) For each project and/or system with which information will be shared, describe why information is shared.
4) For each project and/or system with which information will be shared, describe who will be responsible for protecting the privacy rights of the individuals whose data will be shared across this interface.

Other User(s)
No

If information is shared with persons or organization(s) that are not described by the categories provided, use this field to identify and describe what other persons or organization(s) have access to personal information stored on project systems. Also, briefly describe the data sharing.

6.1.a.1) Describe here who has access to personal information maintained in project's IT systems:
Local issuance site Enrollment Officer and Issuance Officers will manage the secure storage of data captured in the HSPD-12 Probaris system. They also have access to the same information stored at Data Centers on the PIV Web-based electronic enrollment forms. Only the Registrar, Issuers, Sponsors (for reviewing their data input), system administrators, and Tier II and III maintenance operations have access to the data maintained in the PIV system.

6.1.b) How is access to the data determined?
The Security Service of the USPTO PIV System is a critical component that protects sensitive, privacy, and agency-restricted data. This provides the compliance mechanism for the Federal Information Security Management Act 2002 (FISMA) and provides the

assurance that the data collected, used and stored by the system is protected at an appropriate level to restrict unauthorized access to sensitive information. Access to the USPTO PIV System is controlled through a combination of Role Based Access Control (RBAC). The RBAC services are provided by the PIV Identity Access Management and consists of defined administrative roles that are permitted access on a case by case basis that is determined by the role the individual holds. The access is established through the separation of the applications, polices and procedures (e.g., PCI Plan, SOPs, etc), and RBAC components (e.g., Probaris ID System). Additionally the RBAC model for access control provides a strong "least privilege" method that ensures no single individual can circumvent security controls to initiate changes or modification to system operation. This access control system helps to ensure that no single entity can perform configuration or modification of the system without conducting acts of collusion with other roles and entities. Probaris accounts are centrally managed by the USPTO Security Officer.

Probaris ID does allow real time auditing via the summary function in any individual's cardholder account. All transaction/life cyle histories are kept and viewable. Information flow within the USPTO PIV System is permitted based upon successful matching of identity, access rights validation, and function privilege. An entity must be strongly authenticated to provide assurance of the identity of the operator prior to granting access to a function. An authenticated entity must have approved access rights and the requested function must be appropriate for the role the individual/entity fills to successfully access a requested functionality. Client services are provided with a session lock and session termination security control that is enforced by the PIV Card. After a specific number of incorrect attempts to access the PIV Card, the device will suspend its operation and require administrative intervention to unlock. This lock mechanism mitigates the risk of a brute-force attack to obtain access to privacy and personal data that is stored on the card.

6.1.c) Are criteria, procedures, controls, and responsibilities regarding access documented? If so, identify the documents.

Yes, the criteria, procedures, and responsibilities regarding access are documented in the USPTO PIV system Design Document. In addition, an Operations and Maintenance manual will be provided to Operations personnel at the Data Centers, and an Enrollment Handbook and User Guide will be provided to the PIV administrators documenting access control rights and procedures. Additionally, there is documentation in the USPTO PIV Card Issuers Operations Plan and accompanying SOPs.

6.1.d) Will users have access to all data on the project systems or will user access be restricted? Explain.

Information flow within the USPTO PIV system is permitted based upon successful matching of identity, access rights validation and function privilege. A user, or entity, must be authenticated to provide assurance of the identity of the operator prior to granting access to a function. An authenticated entity must have approved access rights and the requested function must be a appropriate for the role the individual/entity fills to

successfully access a requested functionality. Accordingly, only users having inherent assigned rights to access will be provided access by the system security controls.

6.1.e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by those having access? (Please list processes and training materials that specifically relate to unauthorized browsing)

Consistent with the requirements of the Federal Information
Security Management Act (Pub. L. 107-296) and associated OMB policies, standards and guidance from the National Institute of Standards and Technology, and the General Services Administration, the USPTO Office of Security and Safety protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards.

Access is restricted on a ``need to know'' basis, utilization of HSPD-12 card access, secure network access, and card readers on doors and approved storage containers. The building has security guards and secured doors. All entrances are monitored through electronic surveillance equipment. The hosting facility is supported by 24/7 onsite hosting and network monitoring by trained technical staff. Physical security controls include indoor and outdoor security monitoring and surveillance; badge and picture ID access screening; and pincode access screening. Personally identifiable information is safeguarded and protected in conformance with all Federal statutory and OMB guidance requirements. All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All data is encrypted in transit. The USPTO will maintain an audit trail and perform random periodic reviews to identify unauthorized access. Persons given roles in the HSPD-12 process must be approved by the USPTO and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.

6.1.f) Is personal information shared (is access provided to anyone other than the system users, system owner, Project Manager, System Administrator)? (Yes/No)

Yes

Note: If you have selected No above, then SKIP to question 6.2, "Access to Records and Requests for Corrections".

6.1.g) Identify the measures taken to protect the privacy rights of the individuals whose data will be shared.

The PIV privacy data collected is not shared with externally entities. However, regarding fingerprints collected during PIV enrollment for the purposes of adjudicating criminal background checks for PIV card applicants, OPM and FBI are responsible for protecting the privacy rights of the individuals for fingerprints that are received at their external sites. In addition, the USPTO does not store the captured fingerprints locally. In a future phase of the PIV effort, the fingerprint collection process will be integrated within the PIV

registration process and transmitted to the FBI via the EFT standard. The USPTO has a secure encrypted network connection for data transmission between to the FBI to mitigate any risk of data interception or modification. Accordingly, in the future PIV versions, the Registrar at the USPTO sites is responsible for protecting the privacy rights while collecting the fingerprints, during transmission and prior to OPM receiving their fingerprints results in paper form.

6.1.h) Identify who is responsible, once personal information leaves your project's IT system(s), for ensuring that the information is protected.
The FBI and OPM are responsible for protecting the privacy rights of the individuals for fingerprints that are received and stored at their external sites. They have been managing this fingerprint data from state and federal agencies for many years and have their federal security-approved controls in place.

6.1.i) Describe how personal information that is shared is transmitted or disclosed.
The USPTO has a secure encrypted VPN network connection for fingerprint data transmission to the FBI to mitigate any risk of data interception or modification. OPM submissions are done via sealed envelopes and the U.S. Postal Service, which is authorized to transfer PII (which USPTO has securely sealed via envelope.

6.1.j) Is a Memorandum of Understanding (MOU), contract, or any other agreement in place with all external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.
A MOU is in place between USPTO and DOJ/FBI for their Civil Applicant System (CAS), which is the system where FBI fingerprints are submitted and results received. A System of Records Notice is in place with OPM as fingerprint data is collected and transmitted between USPTO and OPM in paper form such as results or actual fingerprints submissions which OPM will then submit to the FBI on USPTO's behalf.

6.1.k) How is the shared information secured by the recipient?
Both OPM and FBI have their own federally approved policy controls in place for securing shared fingerprint information received from outside agencies.

6.1.l) What type of training is required for users from agencies outside USPTO prior to receiving access to the information?
None. These fingerprint data transmissions are normal ongoing daily operations at OPM and FBI.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

6.2 Access to Records and Requests for Corrections

The Privacy Act and USPTO policy provide certain rights and mechanisms by which individuals may request access to and amendment of information relating to them that is retained in a System of Records.

6.2.a) How can individuals view instructions for accessing or amending data related to them that is maintained by USPTO? (Select all applicable options below.)

No- The application will provide a link that leads to their information.

No- The application will provide, via link or where data is collected, written instruction or how to access/amend their information.

No- The application will provide a phone number of a VA representative who will provide instructions.

Yes- The application will use other method (explain below).

No- The application is exempt from needing to provide access.

6.2.b) What are the procedures that allow individuals to gain access to their own information?

Only during initial PIV enrollment are applicants permitted to view their current privacy data, and in the presence of the PIV Sponsor. There is a USPTO SOP entitled " Access Personal Credential Process SOP."

6.2.c) What are the procedures for correcting erroneous information?

See 6.2b

6.2.d) If no redress is provided, are alternatives available?

Not Applicable

6.2.e) Provide here any additional explanation; if exempt, explain why the application is exempt from providing access and amendment.

Not Applicable

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

7.) Retention and Disposal

By completing this section, you provide documented assurance that proper data retention and disposal practices are in place. The "Retention and disposal" section of the applicable System of Records Notice(s) often provides appropriate and sufficiently detailed documented data retention and disposal practices specific to your project.

USPTO HBK.

System of Records Notices may be accessed here

For VBA projects, Records Control Schedule (RCS) VB-1 provides more general guidance. VBA Records Control Schedule (RCS) VB-1 may be accessed via the URL listed below.

7.a) What is the data retention period? Given the purpose of retaining the information, explain why the information is needed for the indicated period.

The Card Holder's privacy data collected during HSPD-12 Card Registration (PII) is handled in accordance with the data storage and retention policies that are enforced by the associated USPTO System of Record. Current retention policies are to keep electronic badge information for two years after an individual has departed the Agency. HSPD-12 records will be purged after a two year period to keep uniformity between legacy badges and HSPD-12 cards.

7.b) What are the procedures for eliminating data at the end of the retention period?

The IAM Service tracks all data elements within the system and has the ability to tag data that is no longer required in production/operation. these data elements and associated user profile packages are to be archived in accordance with NARA regulations and will be securely provided over the Web services (e.g., HTTPS) to an archive instance that is to be identified by the USPTO.

7.c) Where are procedures documented?

USPTO PIV Card Issuers Operations Plan

7.d) How are data retention procedures enforced?

On a calendar year annual basis, a report is created for all expired/de-activated credentials and they are deleted from the system. This process currently in place for legacy badging will be replicated for HSPD-12 credentials.

7.e) If applicable, has the retention schedule been approved by the National Archives and Records Administration (NARA)?

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

PIV is following the NARA guidelines and USPTO document policies.

8 SECURITY

OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, (OMB M-03-22) specifies that privacy impact assessments must address how collected information will be secured.

8.1 General Security Measures

8.1.a) Per OMB guidance, citing requirements of the Federal Information Security Management Act, address the following items (select all applicable boxes.):

Yes - The project is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured.

Yes- The project has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.

Yes- Security monitoring, testing, and evaluating are conducted on a regular basis to ensure that controls continue to work properly, safeguarding the information.

8.1.b) Describe the security monitoring, testing, and evaluating that is conducted on a regular basis:
The Security Service of the USPTO PIV System is a critical component that protects sensitive, privacy, and agency restricted data. This service provides the compliance mechanism for the Federal Information Security Management Act of 2002 (FISMA) and provides the assurance that the data collected and used and store by the system is protected at an appropriate level to restrict unauthorized access to sensitive information. User Accounts are digitally signed to detect modification and protect the integrity of the system.

8.1.c) Is adequate physical security in place to protect against unauthorized access?
Yes

8.2 Project-Specific Security Measures
8.2.a) Provide a specific description of how collected information will be secured.

- *A concise description of how data will be protected against unauthorized access, unauthorized modification, and how the availability of the system will be protected.*
- *A concise description of the administrative controls (Security Plans, Rules of Behavior, Procedures for establishing user accounts, etc.).*
- *A concise description of the technical controls (Access Controls, Intrusion Detection, etc.) that will be in place to safeguard the information.*

Describe any types of controls that may be in place to ensure that information is used in accordance with the above described uses. For example, are audit logs regularly reviewed to ensure appropriate use of information? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?
Note: Administrative and technical safeguards must be specific to the system covered by the PIA, rather than an overall description of how the USPTO's network is secured. Does the project/system have its own security controls, independent of the USPTO network? if so, describe these controls.

The security of USPTO PIV System is a critical component that protects sensitive, privacy and agency restricted data. Access to the USPTO PIV System is controlled through OCIO access control services. The role based services consist of defined administrative roles that are permitted access on a component per component basis. The Security Service is established through the separation of the applications (Probaris ID) and policies (e.g., SOPS, etc.). By establishing this separation of function, the Probaris ID system has an architecture that does not lend itself to any one component being capable of accessing secure or sensitive data when compromised.

Additionally the role based model for access control provides a strong "least privilege" method that ensures no single individual can circumvent security controls to initiate

changes or modification to system operation. The controls offer split knowledge or split key services that require multiple operators to work together to obtain access to sensitive computing components of the USPTO PIV System (HSM, CMS, etc). This access control ensures that no single entity can perform configuration or modification of the system without conducting acts of collusion with other roles and entities.

Client services are provided with a session lock and session termination security control that is enforced by the PIV Card. After a specific number of incorrect attempts to access the PIV Card, the device will suspend its operation and require administrative intervention to unlock. This lock mechanism mitigates the risk of a brute-force attack to obtain access to privacy and personal data that is stored on the card. In addition, the PKI services that are integrated with the PIV Card support session time-out services. These session time-out services must be implemented in the integrated software and application services that use the PKI services (e.g., digital signature and encryption) and are not within the boundary of the PIV system.

System Integrity Controls

System Integrity Controls help to ensure that information systems are safe from attacks, intrusions, or unauthorized access attempts from both internal and external sources. This section details the system integrity controls employed on the USPTO PIV System.

Encryption

The USPTO PIV System uses a FIPS 140-approved cryptographic module to create encryption keys that support encryption at various levels. Passwords are automatically encrypted when stored. SSL encryption keys are used to secure the transfer off data between system components. The SSH keys are created during the time of the production system installation and configuration and are securely stored on each server. End User/Subscriber encryption key are used to encrypt information and data for users. These encryption keys can be used to secure information in the form of an email, a file, a folder, or grouping of data. These keys are issued to the End User during the registration process. The private decryption key is securely stored on the End Users smart card. The public encryption information is stored in the Shadow Directories to facilitate encrypting communications for other users. The SSP's CA has a master encryption key that is securely stored on the LUNA CA3 HSM (Hardware Security Module). This key never leaves the HSM device and is used to secure information in the CA internal database. Only the SSP's CA is authorized to encrypt/decrypt database information. The Luna RA is a scalable, high-performance, secure key issuance HSM. It offers FI 140-2 level 2 validation with level 3 validated Random Number Generation (RNG) for secure key generation. The Luna RA fully supports the following hashing algorithms: SHA-1, MD-2, and MD-5. Once a card's issuance sequence is complete, the Lana RA destroys the card's private key that is stored on the HSM. This enhances the audit ability of the certificate issuance process.

Intrusion Detection and Prevention

A number of elements included in the USPTO PIV System design will be provided by the USPTO Data Center. These elements include: firewalls and network-based IDS (Intrusion Detection System). Firewall and firewall-based tolls can be configured to detect, block, and notify administrators the intrusion attempts. The firewall units have the ability to detect a number of different attacks, including Denial of Service (DOS) and malformed packet attacks. IDS Network Sensors to protect against malicious network attack that pass through firewall controls by analyzing various network protocols. The IDS product will be placed on all servers to provide real-time intrusion protection and detection. These host-based IDS system will analyzed events, host logs, and inbound and outbound traffic to prevent malicious network attacks.

Virus Protection

Virus detection software is part of the base-build for all USPTO PIV System components. Resident virus scanning is performed on all USPTO PIV System workstations and servers. All local drives and file extensions will be scanned in accordance with USPTO policy. In addition, all inbound files will be scanned as they are moved to the specific component. All media to be installed on the USPTO PIV System must be scanned for known viruses prior to installing such media on the system. n the event that a virus is detected, the virus protection engine will attempt to clean the virus. A message will be sent to an administrator and a log entry noting the virus detection and subsequent actions. In the event that the engine fails to clean the virus, it will best placed into a designated quarantine area on the server and will be available for further investigation.

Prevention of Denial of Service Attacks

The security architecture of the USPTO PIV System significantly reduces the effectiveness of a denial of service attack through the use of load balancers, Shadow Directories, firewalls, and a Disaster Recovery site located at an offsite location. The USPTO PIV System's firewall supports DOS countermeasures. The Firewall Security Appliance scans for more than 55 different attack “signatures" and includes a number of intrusion-prevention features such as Flood guard, DNSGuard, FragGuard, and IPVerify. These tools allow the firewall to look for attacks, block them, and provide real-time notification to administrators. In addition, the USPTO Enterprise IDS solution will be configured by the data centers to trigger an alert for suspicious activity that matches criteria defined by the USPTO.

System Banner Messages

The USPTO PIV System is can only be accessed after a user has logged in and seen the USPTO standard logon banner. Users are not able to proceed with a session until the access banner is acknowledged by clicking the "OK" button on the screen.

Operating System Security

USPTO policy establishes United States Patent and Trademark Office (USPTO) standards for the creation, maintenance and use of secure baselines. USPTO uses a Server Operating System Baseline Configuration (Server OS Baseline) which is: the minimum configuration of an operating system that meets USPTO security and operational requirements. The baseline serves as the starting point for the configuration of different types of servers (ex. Oracle database servers, Portal Application Platform servers, Web Services servers).
The secure baseline configuration was created in accordance with vendor recommendations, Federal regulations, Federal Information Processing Standards (FIPS), NIST recommendations (NIST Special Publication 800-70: Security Configuration Checklists Program for IT Products), DISA Security and Technical Implementation Guides (STIGS) and USPTO policy and operational practices. The secure baseline addresses all aspects of the OS and device configuration including but not limited to:

- **Configuration of USPTO required security controls.**
- **Elimination of unnecessary services and utilities.**
- **Configuration requirements for allowed services and utilities.**
- **Standardization of audit logging configurations.**
- **Application of current vendor recommended patch sets and/or service packs.**

The secure baseline is the minimum configuration for all servers and deployed within USPTO. All HSPD 12 servers and network devices, where practicable, will be updated regularly in accordance with the Server Operating System Patch Management Procedures (IT-212.5-01:TN17). The secure baseline documents will be periodically updated to reflect new security patches installed in accordance with the Server Operating System Patch Management Procedures (IT-212.5-01:TN17) and changes to industry best practices recommendations.

Technical Access Control

Both the Windows 2003 Enterprise Servers and Entrust Authority have been tested and certified as enforcing Discretionary Access Control (DAC). The USPTO PIV System supports the following:
FDP_ACC.1
FDP_ACF.1.1
FDP_ACF. 1.2
FDP_ACF. 1.3
FDP_ ACF. 1.4

The USPTO PIV System identifies specific trusted roles the necessary access to accomplished assigned roles. Technical access controls are provided by the OS Windows 2003. Windows 2003 access control controls access to system resources through local system accounts Strong authentication is supported through the use of certificates and the Windows 2003 Operating System security functions.

Password Management

Password Management Windows 2003 Enterprise supports configuration of password policies by an authorized administrator to meet or exceed the USPTO's requirements. Window 2003 will manage the system passwords for the systems that do not support smart card authentication, SSP's CA, Enterprise Directory and CMS. The systems will strictly use Window 2003 passwords that will be independent of the smart card authentication process. This means the PKI credentials are not being used to logon to the local system or to the network. Users logon to the local system or to the network using their normal Windows 2003 password. The Administrator will only be required to provide the PIN that is used to secure the smart card credentials.

Connections to Non Department Entities:

There are no connections outside USPTO security boundaries for the USPTO PIV System. Where necessary, firewalls are employed to segregate the USPTO PIV System from the rest of the internal USPTO network. No modems are installed.

Operating System Security Auditing

Windows 2000 security audit capability exceeds the level of audit detail specified by the USPTO requirements. The Operating System also supports Protected Audit Trail Storage (FAU-STG.1) and restricts any modification of the audit log to the role of authorized administrators (FMT_MOF.1(a), FMT_MTD.1(a) and FMT_MTD.1(b). These security requirements are referenced in the "Windows 2000 Security Target: ST Version 2.0;" 18 October 2002 from Microsoft. The Security Audit Logs are routinely backed up and stored off-site for 5 years.

8.2.b) Explain how the project meets IT security requirements and procedures required by federal law.

The USPTO PIV Project is a Departmental initiative intended to provide compliance with HSPD-12, FIPS 201-1, the Federal Common Policy, and related standards which address the Federal Government need for a standardized identity (PIV) credential to be issued all Federal employees and contractors. Pertinent legislation and guidance driving PIV include, but are not limited to the HSPD 12, FIPS 201-1, OMB M-05-24, E-Government Act of 2002, FISMA/GISRA legislation, the Government Paperwork Elimination Act (GPEA), HIPAA, OMB and National Institute of Standards and Technology (NIST) guidance, and Government Accounting Office (GAO) reports on USPTO security. Further, PIV program management will work with the PKI Entrust Service Provider. The Federal Identity Credentialing Committee has mandated the use of a PKI Federal Bridge Service Provider and conformance to the Federal Common Policy. The PIV System is using an approved PKI Service Provider and is in compliance with the Federal Common Policy. FIPS-201 defines the requirements for the PIV credential enrollment and issuance processes necessary to provide a common assurance level under which all PIV credential are issued. The USPTO PIV System will implement PIV Card, PKI and Identity and Access Management services to meet the requirements of FIPS 201-1. The USPTO PIV System automates the enrollment and issuance process for the PIV credential, manages the

identities of PIV cardholders, manages the lifecycle of the PIV credential, provides data management and provisioning services for interfacing systems, and provides audit and reporting data on PIV System transactions and events. System Integrity Controls help to ensure that information systems are safe from attacks intrusions, or unauthorized access attempts from both internal and external sources. Here are some examples that identifies how the project meet IT Security Requirements required by federal law:

Encryption
The USPTO PIV System uses a FIPS 140 approved cryptographic module to create encryption keys that support encryption at various levels. Passwords are automatically encrypted when stored encryption keys are used to secure the transfer of data between system components. The keys are created during the time of the production system installation and configuration and are securely stored on each server. The federally approved SSP's CA has a master encryption key which is securely stored on the. Only the SSP's CA is authorized to encrypt/decrypt database information. The RA is a scalable, high performance, secure key issuance HSM which offers FIPS 140-2 level 2 validation with level 3 validated Random Number Generation (RNG) for secure key generation, supporting the following NIST approved hashing algorithms.
Security Subsystem
The Security Sub-system of the USPTO PIV System is a critical component that protects sensitive, privacy, and agency restricted data. This sub-system provides the compliance mechanism for the Federal Information Security Management Act of 2002. (FISMA) and provides the assurance that the data collected and used and stored by the system is protected at an appropriate level to restrict unauthorized access to sensitive information.

9. CHANGE

OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, mandates that PIAs address any project/ system changes that potentially create new privacy risks. By completing this section, you provide documented assurance that significant project/ system modifications have been appropriately evaluated for privacy-related impacts.

9.a Since the last PIA submitted, have any significant changes been made to the system that might impact the privacy of people whose information is retained on project systems? (Yes, No, N/A: first PIA)
No

If no, then proceed to Section 10, “Children’s Online Privacy Protection Act.”
If yes, then please complete the information in the table below. List each significant change on a separate row. ‘Significant changes’ may include:
Conversions - when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;

Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:• For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:• For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public; Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement); New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA; Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form: • For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.

Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information);

List All Major Project/System Modification(s)	State Justification for Modification(s)	*Concisely describe:	Modification Approver	Date

* The effect of the modification on the privacy of collected personal information. How any adverse effects on the privacy of collected information were mitigated.

10. CHILDREN’S ONLINE PRIVACY PROTECTION ACT

10.a) Will information be collected through the Internet from children under age 13?
No

If “No” then SKIP to Section 11, "PIA Considerations".
10.b) How will parental or guardian approval be obtained.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

11. PIA CONSIDERATIONS

11) Identify what choices were made regarding the project/system or collection of information as a result of performing the PIA. Examples of choices made include reconsideration of: collection source, collection methods, controls to mitigate misuse of information, provision of consent and privacy notice, and security controls.

This is the second PIA performed on the PIV system. Future considerations to subsequent PIV system design or operations will be made with full consideration of IA impact.

ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

12. PUBLIC AVAILABILITY

The Electronic Government Act of 2002 requires that USPTO make this PIA available to the public. This section is intended to provide documented assurance that the PIA is reviewed for any potentially sensitive information that should be removed from the version of the PIA that is made available to the public.

The following guidance is excerpted from M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Section II.C.3, "Review and Publication": iii. Agencies must ensure that the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment.. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

12.a) Does this PIA contain any sensitive information that could cause harm to the USPTO or any party if disclosed
to the public?
No

12.b) If yes, specify:
ADDITIONAL INFORMATION: (Provide any necessary clarifying information or additional explanation for this section.)

SIGNATORY AUTHORITY

Agreed: ______________________ 4 / 11 / 11

Joseph Burns Date

Information System Owner

Agreed: ______________________ 4 / 29 / 11

Rod Turk Date

Senior Agency Information Security Officer

Agreed: ______________________ 4 / 15 / 11

Patricia M. Richter Date

Authorizing Official

Add additional signature authorities necessary for the PIA process at your Operating Unit; otherwise, delete this text.